LESSONS LEARNED: SEPTEMBER 11

A Business Continuity Approach

Barbara Allen
SunGard Planning Solutions
December 11, 2002

Pre 9/11 Disaster Trends

Most continuity plans assumed……

- A worst-case scenario where one or more buildings become inaccessible or destroyed by fire or similar level of disaster
- Key staff will still be available
- Primary suppliers will be unaffected
- Utilities will be available
- Recovery will be able to begin within days if not sooner
- Backups of critical data are available and can be recovered
- “Luck” will play a part in the recovery

9/11 Facts……

- **Communications difficult, if not impossible**
- **Staff not available for recovery**
- **Lack of meeting places and command centers**
- **Alpha paging to cell phones worked**
  - **Messaging to pagers worked well**

Terrorism and Business Continuity Planning

- **Unique Challenges**
- **Loss of Life**
- **Transportation Lockdown**
- **Records and Information Loss**
- **Telecommunications Failure**
- **Size of Affected Area**

People Issues are Paramount

- **Safety and Security**
- **Cannot assume survival of key personnel**
- **Trauma and stres**
  performance duri
- **Families come firs**

Protect Human Resources

Emergency Supplies

- Flashlights
- Hard Hats
- First Aid Kits
- Oxygen / Filter Masks
- Goggles
- Battery-powered Radios
- Batteries

Protect Human Resources

Incident Management Planning Works!

- Default Assembly and Coordination Locations (local & remote)
- Notification and Escalation
- Preplanned Decision Making Process
- Public Relations Strategy

Things to Consider as a Result of September 11, 2001

- **Testing**
  - **Create a recovery strategy and test it**
  - **Do not test in a vacuum; test the way you intend to recover, recover the way you test; test to the point of recovery**
  - **Test to identify areas of improvement**
- **Awareness**
  - **Prevention**
  - **Protection**
- **Staff**
  - **Use backup staff to recover**
  - **Be ready to deal with the human side of disaster**

Disaster Recovery - Data is the key

- **How long can you live without it?**
- **How long to restore the data?**
- **How much (if any) can you afford to lose?**
- **Recovery timelines – prioritization**
  - **Not all applications and data need to be recovered at the same time but…**
  - **Be sure to identify *all* interdependencies in advance of a disaster**
  - **Minimize data loss**
  - **Protect your critical records**

September 11, 2002

“The attack on the World Trade Center is something no one could have anticipated and no one could have planned for…”

- **TRUE**
- **FALSE**

September 11th – Our Wake Up Call

- **A New Perspective**
- **Increased Awareness**
- **Expansion of Recovery Responsibilities**
- **Potential Attacks**
  - **Physical**
  - **Cyber (Increasing treat)**

How well do you know your business?

- **Critical Functions**
- **RTOs and RPOs**
- **Interdependencies**

Lessons Learned – Plan Well

- **Access needs and criticalities**
- **Document policies and plans**
- **Revisit your plan and recovery requirements often**
- **Consider the process or function you need to recover – not just the information, data and records**

Test Your Plan – Train Your People

- **Make testing and training a priority**
- **Test the way you recover and recover the way you test**
- **Maintain and update your plans**
  - **Reassess strategies and assumptions**
  - **Update resource data**
  - **Update procedures**
  - **Validation and awareness training**

Disperse and Diversify

- **Don’t put all your eggs in one basket**
- **House intellectual capital and personnel in alternate or multiple sites**
- **Evaluate off site storage**
  - **Frequency**
  - **Completeness**

Take a Holistic Approach

- **Organization wide planning**
- **Standardization**
- **Full life cycle planning**
- **Aggressive security planning – a threat that should not be forgotten**

SUNGAR
D

-The Lesson Learned -
Disasters Happen

Be Prepared To Respond and Recover